Statement of Mike Sicilia, Executive Vice President, Industries
Oracle Corporation

Before the

U.S. House
Committee on Veterans' Affairs
Subcommittee on Oversight and Investigations
Subcommittee on Technology Modernization

Hearing on

"Protecting the Privacy of Veterans' Data"

December 14, 2022

Introduction:

Chairman Pappas, Ranking Member Mann, Chairman Mrvan, Ranking Member Rosendale, and members of the Subcommittees, thank you for the opportunity to speak with you today about Oracle's role in protecting the privacy and security of veterans' Electronic Health Record (EHR) data through our work with the Department of Veterans Affairs' (VA) Electronic Health Record Modernization (EHRM) program.

I am Mike Sicilia, Executive Vice President for Industries at Oracle. I am responsible for Oracle's Global Health Business Unit, including Oracle Cerner.

As you know, Oracle acquired Cerner in June of this year and assumed Cerner's responsibilities under its EHRM contract with VA. In so doing we have taken on the important responsibility of securing the health data and protecting the privacy of our nation's veterans. Oracle's core competence for nearly 40 years is ensuring the security of much of the world's most important data – from government to critical infrastructure like utilities to banking to telecommunications and healthcare.

Data security and data privacy are two sides of the same coin, and I would like to address each in turn. Let me tackle the easier topic first, privacy.

Privacy of Veterans' Health Data

I want to start with foundational framing. Data privacy has been a big topic of debate around the collection, use, and monetization of consumer data, particularly by so-called "big tech." I want to emphasize that Oracle has been on the record for years in favor of stronger consumer privacy protections in general and is in support of guaranteeing the strong protection of health data for all Americans, including our nation's veterans.

First, and most importantly, veterans are protected – like all our citizens by the Health Insurance Portability and Accountability Act (HIPAA). HIPAA provides a baseline of protection for individual's health information and has been in place since 1996. That law – which is the purview of Congress – aims to balance the protection of personal health information and the use of healthcare data to improve patient outcomes and protect the public's health. HIPAA creates a special category of protections – "protected health information" – and establishes limits and rules protecting against use and disclosure of this data without an individual's express authorization. Specifically, in this regard, the EHRM system being implemented for VA enables HIPAA compliance, and we have substantial experience in securing personal health data in our clinical trials cloud. Put simply, personal healthcare data is owned and controlled by patients.

Second, in the context of VA and an EHR generated within VA's health system (or the Department of Defense (DoD) or Coast Guard), the personal data is owned and controlled by VA as both the healthcare provider and the administrator of the VA health plan.

Under no circumstance is *any* of the personal data within a VA patient's electronic medical record owned by Oracle or viewed by, or accessed by Oracle for our own or any other purposes except for purposes of providing the services specified by the VA contract.

To this end, Oracle's contract with VA is explicit about the ownership of EHR data, stating that "EHRM Data is the exclusive property of the U.S. Government." For reference the relevant section of the contract is attached as Appendix A.

When veterans receive care outside the VA network at community care centers, the Oracle Cerner EHR system facilitates the sharing of that veteran's electronic medical record. This data sharing is limited and necessary to ensure a veteran receives the best care when outside of VA's network and occurs under strict controls and adherence to applicable legal requirements. But even with permission to share data in this instance, Oracle does not gain any new access, visibility or rights for the data.

More generally, Oracle's relationship with patient data in our EHR system is identical to the relationship with our customer's data in our accounting systems or human resources (HR) systems. Even though hundreds of thousands of Oracle customers store accounting or HR data in Oracle systems, under no circumstances may we access *any* of that information for purposes other than at the express direction of the customer. We cannot, for example, de-identify millions of HR records and run analytics or machine learning against this data and "productize" or "monetize" aggregate HR trends. Likewise, we cannot and do not access the financial entries in Oracle accounting systems in use by our customers. In exactly the same way, Oracle cannot and does not access medical records stored in *any* EHR system commercial or government operated unless the customer has specifically directed us to do so.

Oracle's relationship with our customers' data is exactly like other technology companies you use every day. Join a video conference over Zoom and record the meeting – Zoom does not participate in the meeting or own your recording. Send your colleague a Word document with your confidential business plan – Microsoft does not own or access your document. As a technology provider of tools and systems for our customers, in VA's case an EHR system, Oracle does not own the work product of our customers, or the data our customers store in our systems.

While Oracle does have an extremely small, completely unrelated, data brokerage business, this data is *not* collected from our systems but is typically acquired from others. This contrasts with services like YouTube or Facebook, for example, where Google and Meta are the owners

of the customer data and may monetize that information however they see fit, typically through advertising.

Lastly, as you may know, we have been on record – and we believe there should be a public debate – around the use of health information to improve patient outcomes, enhance early detection, cure diseases, share treatment best practices, deal with health crises' like COVID-19, and reduce healthcare costs. With rapid advances in analytics and machine learning, technology can play a key role in helping to improve global healthcare. While we believe this is a critically important public discussion to have, I want to emphasize that it is well beyond the scope of anything contemplated in the VA EHRM program.

In summary, there are tight controls against any usage or sharing of the data by Oracle beyond the sharing of the data as prescribed by the VA contract. Any exception must be explicitly approved and authorized by VA or other federal customers. Oracle is not permitted under its contract and does not seek to monetize veterans' EHR data in any way.

Securing the Data of our Nation's Veterans

The other side of the privacy and security coin is security. I say this is the harder of the two topics because unlike privacy, which operates under a statutory and contractual framework, security assumes there are bad actors (inside and external threats) who may seek to exploit system vulnerabilities for profit or to do harm. At Oracle we architect our systems with the assumption they are under persistent cyber-threat, both at the perimeter and from insiders.

Here, the security of our systems and our customers' data is a core competency of Oracle, which we have architected into our systems from the ground up, from silicon, through operating systems, database and the applications layer. Oracle has decades of experience securing mission critical systems around the world. Security is an area where Oracle brings substantial expertise to the existing capabilities of Cerner.

Within the U.S. government federal space, Oracle holds a number of DOD security accreditations and FedRAMP authorizations, and we are an approved vendor under the Intelligence Community's Commercial Cloud Enterprise (C2E) program and the DoD's Joint Warfighting Cloud Capability (JWCC) program.

Protecting Against Insider Threats

Specific to the VA EHRM, Oracle employees and subcontractors with physical or logical access to the EHR data are required to undergo extensive compliance training annually and in many cases these employees are required to be U.S. citizens who have completed favorable background investigation adjudications. Depending on the employee's role or responsibility

Personal Identity Verification (PIV) or Common Access Cards (CAC) must be used to verify the employee's identity before accessing the system. All of these and additional security requirements align with NIST 800-53.

To ward off an insider threat of accessing EHR data improperly, Oracle and the DHA, utilize monitoring software that audits all data access including reading and modification of medical records in the EHR databases. This is a net new protection and capability far above VistA. VA and DoD also have the ability to audit unauthorized data access or sharing. Taken together, this auditing along with our employee vetting and training work to minimize the possibility of insider threats.

In addition, EHRM adds additional protection in this regard by layering in role-based access to patient data. This shift from a single door for all users from administrative staff to physicians into system data to one based on the data need of the user raises the bar for VA data protections against one of the most common threats.

The Federal Enclave

As we discuss who has access to the EHR data and how it is protected, it is helpful to understand where the EHR data is held: the federal enclave.

In 2015, DoD awarded Leidos a contract to implement the then-Cerner EHR for DoD's health system. Cerner's data center was utilized for the DoD work. In 2018 when VA awarded Cerner the EHRM contract a decision was made for VA to also use the Cerner data center. This data center is now the federal enclave, and it holds federal EHR data for VA, DoD, Coast Guard and other federal users.

Oracle as the new owner of Cerner operates the federal enclave with Leidos under Authorities to Operate (ATO) and Authorities to Connect (ATC) issued by DoD's Defense Health Agency and reciprocally recognized by VA.

As DoD was the first customer, its security standards and requirements were those originally followed, and DoD is critical to the security efforts. After VA joined the federal enclave, an analysis was performed to make sure the most stringent security posture is followed between DoD and VA's varying requirements. Oracle always follows the highest security requirement so in cases where the higher requirement is DoD's, the VA's EHR receives greater security than it would if not being operated jointly in the federal enclave.

Within the federal enclave, DoD and VA control configuration management and other changes and overall security is managed jointly by the DoD, VA, Oracle and Leidos teams working together to monitor and react to all actual and anticipated cyber threats.

The Defense Health Agency monitors all data entering or exiting the federal enclave and controls access points to the federal enclave independently of Oracle and Leidos. As a backstop, DoD always can lock down access to the federal enclave entirely if necessary to thwart a threat.

Securing the Federal Enclave

In terms of network security for the federal enclave, DoD owns and manages the network security stack that controls all traffic in and out of the enclave. Oracle provides additional security monitoring capabilities for the network, and provides host-based security services.

DoD and VA have engaged the Naval Information Warfare Center (NIWC) to provide cybersecurity services for the federal enclave. Oracle jointly works with NIWC to monitor the federal enclave for any cyber intrusions. Cyber penetration testing is conducted by DoD and outside vendors, and all systems within the federal enclave are scanned for vulnerabilities daily.

Vulnerabilities may be found or Oracle may be notified of vulnerabilities by vendors or other government cybersecurity agencies, and when this occurs there are strict remediation timelines for applying fixes.

All subcontractors or third-party vendors to the federal enclave must comply with the same security controls and data access requirements as Oracle.

I can't emphasize enough that shifting from 130 VistA instances and DoD's previous 30 instances of ALHTA to a single system with a uniform cyber security posture across VA and DoD EHR data provides many benefits and enhances cyber defense. This EHR modernization effort leverages cost and programmatic efficiencies, reduces the cyber-attack surface area, removes a major barrier to interoperability and patient data flow, all while enhancing VA and DoD ability to innovate and modernize to stay ahead of evolving cyber security threats.

The bottom-line is that the federal enclave is setup with very stringent security protocols and extensive monitoring and auditing to protect against outside cyber threats and insider threats, and we believe that veterans should have confidence that their EHR data stored in the federal enclave is secure.

Preparing for Future Threats

I have mentioned before Oracle's desire to eventually work with VA, DoD and Leidos to move the EHR workloads to Oracle Cloud Infrastructure (OCI).

OCI is a hyperscale cloud with security built in from the ground up. OCI hosts the data and applications of thousands of commercial and government clients, including dedicated government security regions engineered to host Top Secret data and workloads.

OCI was built with its foundation in scalability and security, and it is compliant with major certifications to include PCI-DSS as well as FedRAMP authorizations. Security is also fully integrated in OCI, with features such as bastions for zero trust access, security zones for compartmentalized workloads and integration of security across the Infrastructure, Database and Application Layers.

Moving to OCI will provide even better protection against future threats, and we hope to eventually receive permission to make this happen.

Closing

My message to the Committee is that on privacy we are responsible stewards of our veterans' data. We do not own or monetize this veterans' data, and we do not use any of it outside of the express permission of VA and the terms of the VA contract. On security, we provide industry leading assurance that data in our systems – including the federal enclave – is protected and secure. And going forward – as we move the EHR to the cloud with the permission of VA and DoD – security will only be enhanced.

We are confident our veterans' EHR data is private, protected, secure and safe. Thank you.

Appendix A

Relevant EHRM Contract Language:

H.7 EHRM DATA CLAUSE

EHRM Data includes, but is not limited to, all healthcare data generated by VA staff, VA devices, instruments, internal and external labs, VA facilities, patients, patient generated data, third-party providers that send data to VA (directly or through a patient), as well as analytics data, reports, studies, analyses, whether in draft or final form, in electronic, print, or other form, prepared by the Contractor or Government, and working papers associated with any of the above, relating in any way to the VA healthcare enterprise and VA implementation of the EHRM under this contract. However, EHRM Data does not include the Contractor's commercial tools and analysis, and Contractor proprietary information related to implementation and delivery of the VA EHRM Solution.

EHRM Data is the exclusive property of the U.S. Government and shall be fully available to the Government subject to current encryption requirements and joint DoD/VA governance, portable by the VA after contract award with sufficient notice to Contractor for packaging and segmenting EHRM Data. EHRM Data will be provided to the Contractor for the Contractor to administer the services set forth in this contract. Except for the third party licensors whose licenses are attached to the Cerner End User License Agreement (Section D of the contract) EHRM Data shall not be sold, licensed, analyzed, or shared with any other persons, organizations, or entities without the express written permission of the VA. EHRM Data modified, updated, revised or changed in any manner by the Contractor during performance of the contract is Technical Data as that term is defined in FAR 52.227-14 (a), Rights in Data—General (May 2014) and VA shall have access to EHRM Data and such Technical Data produced by the Contractor after contract award. Such Technical Data generated, stored, and processed by the Contactor pursuant to this Contract may contain both Sensitive Information and Personally Identifiable Information (PII) and/or Protected Health Information (PHI) of Veterans such that the disclosure thereof would violate the right of privacy or publicity of the individual to whom the information relates or the right of privacy and publicity of the VA. Accordingly, the Contractor relinquishes the rights set forth in FAR 52.227-14 (b) (2) for all such Technical Data delivered to the Contracting Officer (CO).

The CO, in accordance with VA Departmental procedures, will be the sole authorized official to release verbally or in writing, any EHRM Data, such Technical Data described above or any other written or printed materials pertaining to the VA that are maintained and provided by the Contractor pursuant to the requirements of the contract. The Contractor will not release any such information without the express written permission of the VA. At the conclusion of the Contract, and in accordance with PWS 5.13, the Contractor shall return to VA, in a format

acceptable to VA, all EHRM Data, and such Technical Data described above, generated and processed by the Contractor in performance of this Contract in order that such EHRM Data and Technical Data can be used, stored, and maintained by the Government. Following successful completion of the PWS 5.13 Transition procedures and written instruction from the CO, the Contractor shall also delete all copies, in whole or in part, and any other documents or records derived from EHRM Data.